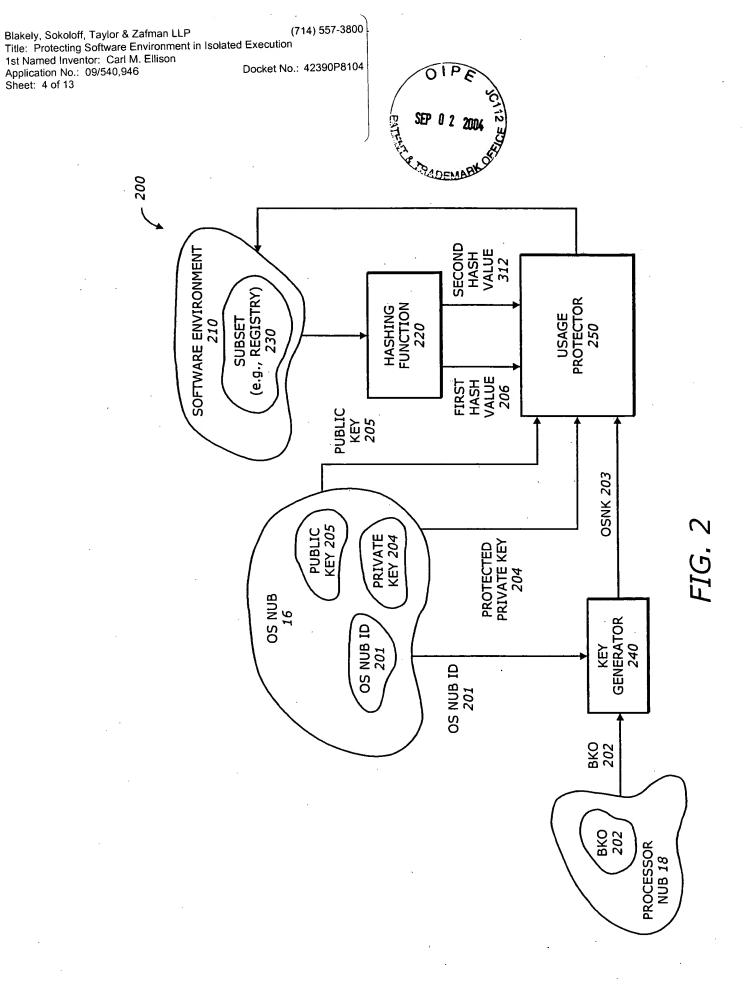
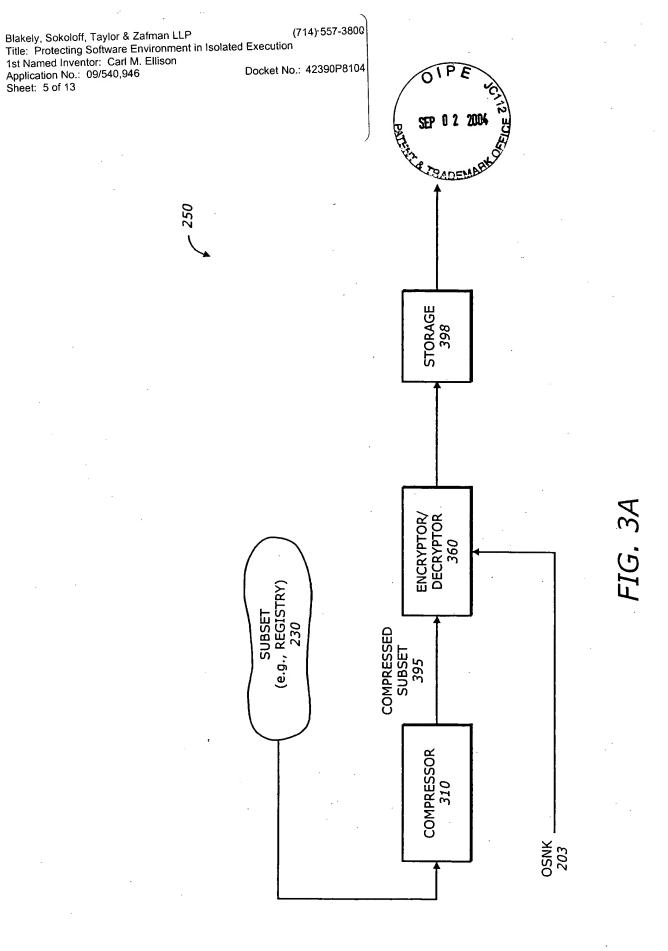


FIG. 1B

(714) 557-3800 Blakely, Sokoloff, Taylor & Zafman LLP (Title: Protecting Software Environment in Isolated Execution SEP 0 2 2004 NU 1st Named Inventor: Carl M. Ellison Docket No.: 42390P8104 Application No.: 09/540,946 Sheet: 3 of 13 100 ACCESSIBLE PHYSICAL MEMORY 60 186 HARD DRIVE TOKENS CD ROM FLOPPY 148 TOKEN 184 STORAGE DEVICE ISÓLATED AREA ISOLATED CONTROL AND STATUS EXECUTION MASS ISOLATED 1 MOTHER-BOARD TOKEN 170 1 156 1 182 **EXECUTION** 140 155 NORMAL CRYPTOGRAPHIC KEY STORAGE LOADED OS LOGICAL PROCESSING SYSTEM MEMORY 156 EXECUTION MANAGER ISOLATED 1 180 HOST BUS 150 TOKEN BUS INPUT/OUTPUT CONTROLLER HUB (ICH) 52 PROCESSOR 120 INTERFACE ISOLATED DIGEST MEMORY BUS 130 MEMORY CONTROLLER 154 PROCESSOR AREA ISOLATED 159 PROCESSOR NUB/ EXECUTIVE LOADER TOKEN BUS INTEFACE HUB (MCH) 110b PROCESSOR 160 110a 175 NON-VOLATILE NUB/ EXECUTIVE I/O DEVICES FIG. 1C PROCESSOR MEMORY

18





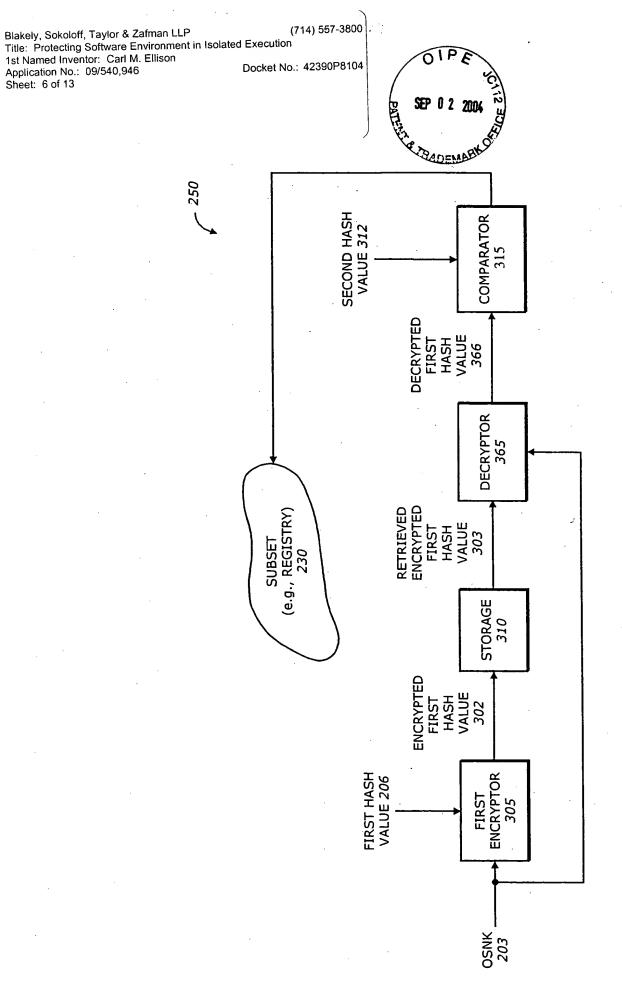
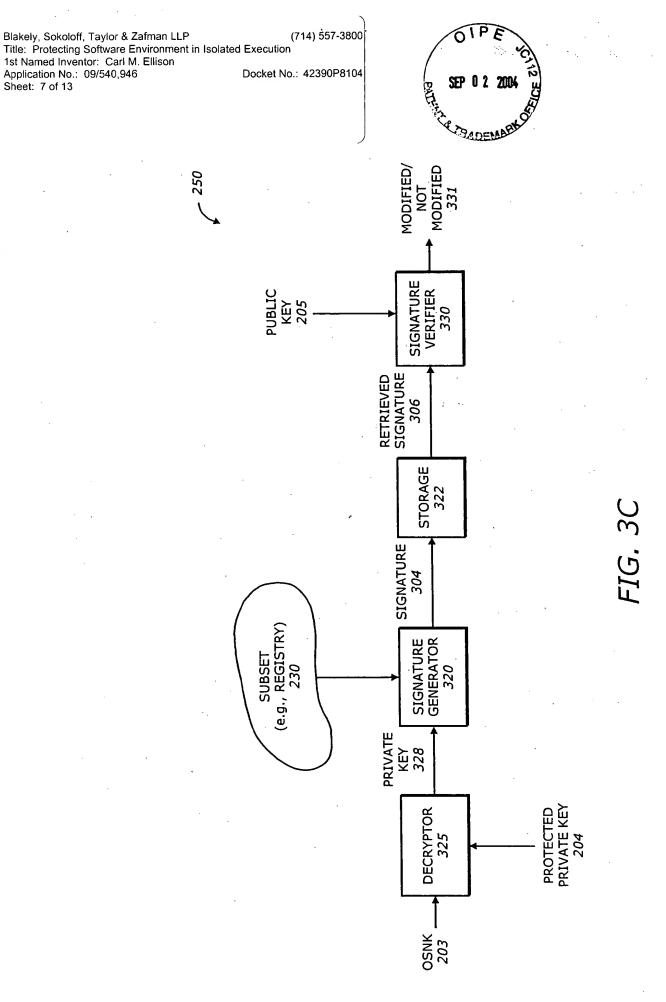


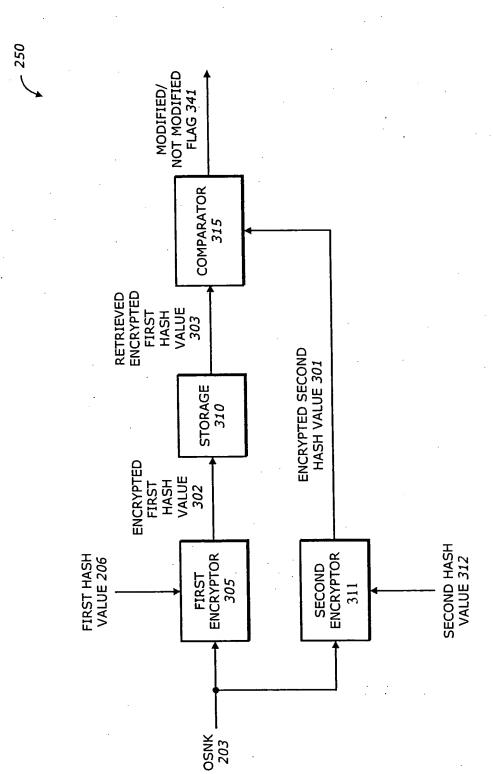
FIG. 3B



Blakely, Sokoloff, Taylor & Zafman LLP (7
Title: Protecting Software Environment in Isolated Execution
1st Named Inventor: Carl M. Ellison (714) 557-3800 Application No.: 09/540,946 Sheet: 8 of 13 Docket No.: 42390P8104 DA DEMARK 250 PASS/ FAIL 358 TEST CENTER 357 SIGNATURE VERIFIED FLAG 351 MANIFEST VERIFIED FLAG 356 PUBLIC KEY 205 SIGNATURE MANIFIEST VERIFIER 355 VERIFIER 350 RETRIEVED SIGNATURE RETRIEVED MANIFEST SUBSET (e.g., REGISTRY) 230 309 354 STORAGE 349 MANIFEST 307 GENERATED SIGNATURE 308 PRIVATE KEY 348 PROTECTED (ENCRYPTED) PRIVATE KEY 204 GENERATOR 335 SIGNATURE GENERATOR 340 DECRYPTOR MANIFEST 345 OSNK 203

Blakely, Sokoloff, Taylor & Zafman LLP (714) 557-3800
Title: Protecting Software Environment in Isolated Execution
1st Named Inventor: Carl M. Ellison
Application No.: 09/540,946 Docket No.: 42390P8104
Sheet: 9 of 13





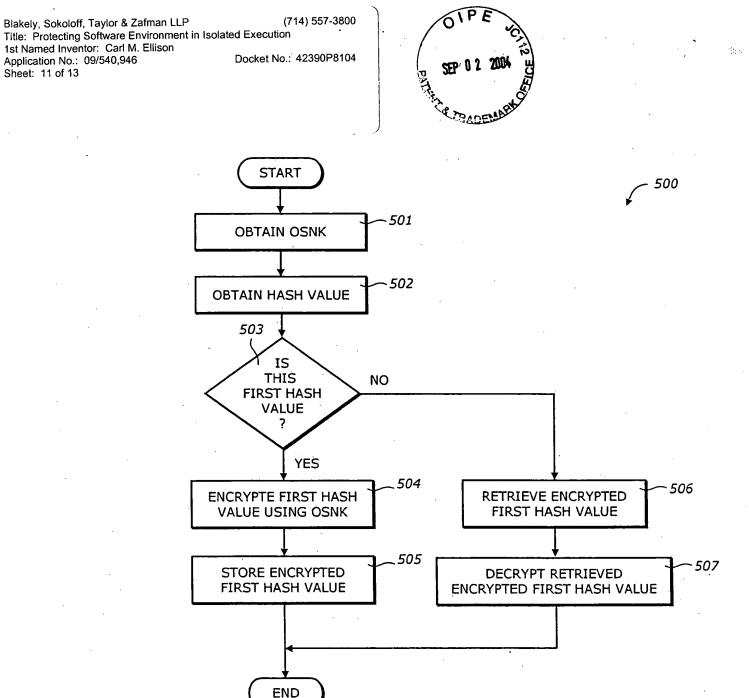
(714) 557-3800 Title: Protecting Software Environment in Isolated Execution Docket No.: 42390P8104 400 **START** 401 **DOES SUBSET** NO **NEED PROTECTION** YES 402 **OBTAIN OSNK** AND SUBSET 403 IS **READING OF** NO SUBSET **AUTHORIZED** YES -404 405 **ENCRYPT SUBSET DECRYPT SUBSET USING OSNK USING OSNK** 406 **STORE DECRYPTED** SUBSET IN STORAGE -407 **RETRIEVE** DECRYPTED SUBSET TO READ THE SUBSET **END**

Blakely, Sokoloff, Taylor & Zafman LLP

1st Named Inventor: Carl M. Ellison Application No.: 09/540,946

Sheet: 10 of 13

FIG. 4



Blakely, Sokoloff, Taylor & Zafman LLP (714) 557-3800 Title: Protecting Software Environment in Isolated Execution 1st Named Inventor: Carl M. Ellison Application No.: 09/540,946 Docket No.: 42390P8104 Sheet: 12 of 13 600 **START** -601 **OBTAIN THE OSNK** - 602 **OBTAIN THE PROTECTED** (ENCRYPTED) PRIVATE KEY 603 DECRYPT THE PROTECTED PRIVATE KEY USING THE OSNK - 604 GENERATE A SIGNATURE FOR THE SUBSET USING THE PRIVATE KEY 605 STORE THE SIGNATURE IN A STORAGE 606 OBTAIN THE PUBLIC KEY

FIG. 6

VERIFY THE SIGNATURE USING THE PUBLIC KEY

GENERATE A MODIFIED/ NOT MODIFIED FLAG

END

607

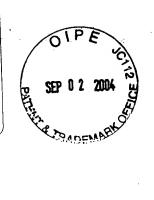
608

(714) 557-3800 Blakely, Sokoloff, Taylor & Zafman LLP Title: Protecting Software Environment in Isolated Execution 1st Named Inventor: Carl M. Ellison

Application No.: 09/540,946

Sheet: 13 of 13

Docket No.: 42390P8104



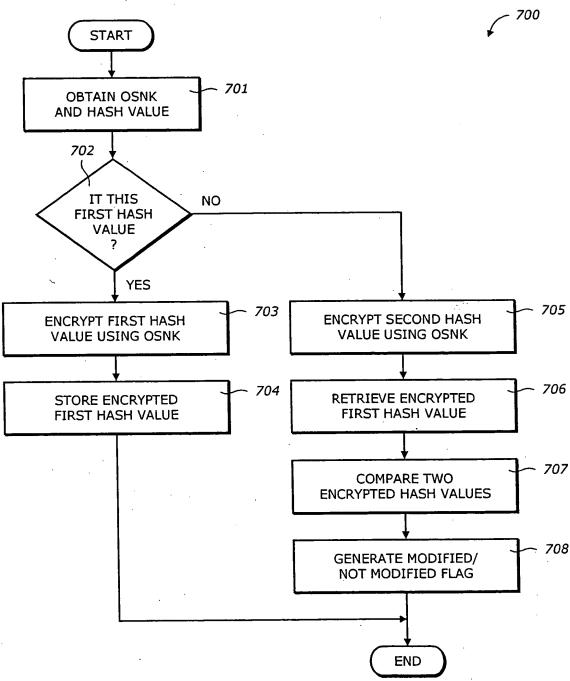


FIG. 7